Docket No. 247971US2TTC RD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Shinobu FUJITA, et al. GAU:

SERIAL NO: New Application EXAMINER:

FILED: Herewith

FOR: SEED GENERATING CIRCUIT, RANDOM NUMBER GENERATING CIRCUIT, SEMICONDUCTOR INTEGRATED CIRCUIT, IC CARD, AND INFORMATION TERMINAL EQUIPMENT

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-019732	January 29, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

1393596505A47

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月２９日

出願番号
Application Number: 特願２００３－０１９７３２

[ST. 10/C]: [ＪＰ２００３－０１９７３２]

出願人
Applicant(s): 株式会社東芝

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７４７９

【書類名】　特許願
【整理番号】　PTS0234
【提出日】　平成15年 1月29日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　7/58
【発明の名称】　シード生成回路、乱数生成回路、半導体集積回路、ＩＣカード及び情報端末機器
【請求項の数】　13
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　藤田　忍
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内
【氏名】　岩村　鉄郎
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100088487
【弁理士】
【氏名又は名称】　松山　允之
【選任した代理人】
【識別番号】　100108062
【弁理士】
【氏名又は名称】　日向寺　雅彦

【手数料の表示】

【予納台帳番号】　087469

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　シード生成回路、乱数生成回路、半導体集積回路、ＩＣカード及び情報端末機器

【特許請求の範囲】

【請求項１】

連続的または断続的に発振する発振回路と、

前記発振回路から出力されたデジタルデータ列における「０」と「１」との出現頻度を制御して時系列データとして出力する平滑回路と、

前記時系列データのうちの複数のビットを用いた演算処理により、１ビットのシードを生成する真性化回路と、

を備えたことを特徴とするシード生成回路。

【請求項２】

前記発振回路は、入力された複数のデータが特定の組み合わせとなった場合のみ発振することを特徴とする請求項１記載のシード生成回路。

【請求項３】

前記発振回路は、２つの排他的論理和演算回路と２つの反転回路をそれぞれ交互に直列接続し、前記２つの排他的論理和演算回路のそれぞれの入力の一端に、前記複数のデータのそれぞれを与えるものであることを特徴とする請求項２記載のシード生成回路。

【請求項４】

前記発振回路は、リング発振回路を含み連続的に発振することを特徴とする請求項１記載のシード生成回路。

【請求項５】

前記平滑回路は、

擬似乱数を生成する擬似乱数生成手段と、

前記発振回路から出力された前記デジタルデータ列と、前記擬似乱数生成手段により生成された前記擬似乱数と、の排他的論理和を演算して前記時系列データとして出力する論理演算手段と、

を有することを特徴とする請求項１～４のいずれか１つに記載のシード生成回

路。

【請求項６】

前記平滑回路は、その出力において、前記発振回路から出力されたデジタルデータ列よりも「０」と「１」との出現頻度が１：１に近いことを特徴とする請求項１～５のいずれか１つに記載のシード生成回路。

【請求項７】

前記真性化回路は、前記演算処理を行う排他的論理和演算回路を有することを特徴とする請求項１～６のいずれか１つに記載のシード生成回路。

【請求項８】

前記真性化回路は、前記複数のビットの組み合わせに応じて「０」及び「１」のいずれかを割り当てるテーブルに基づいて前記１ビットのシードを生成することを特徴とする請求項１～６のいずれか１つに記載のシード生成回路。

【請求項９】

請求項１～８のいずれか１つに記載のシード生成回路と、

前記シード生成回路により生成された前記シードに基づいて擬似乱数を生成する擬似乱数生成回路と、

を備えたことを特徴とする乱数生成回路。

【請求項１０】

デジタル入力値に対して一義的に決定されないデジタル出力値を与える不確定論理回路をさらに備え、

前記擬似乱数を前記不確定論理回路に入力して、その出力を乱数として出力することを特徴とする請求項９記載の乱数生成回路。

【請求項１１】

請求項９または１０に記載の乱数生成回路を備えたことを特徴とする半導体集積回路。

【請求項１２】

請求項１１記載の半導体集積回路を備えたことを特徴とするＩＣカード。

【請求項１３】

請求項１１記載の半導体集積回路を備えたことを特徴とする情報端末機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、シード生成回路、乱数生成回路、半導体集積回路、ＩＣカード及び情報端末機器に関し、特に、デジタル論理回路によりコンパクトに構成することが可能でしかも真性度が高い乱数のシードを生成し、暗号アルゴリズムに用いても好適なシード生成回路及びこれを用いた乱数生成回路、半導体集積回路、ＩＣカード及び情報端末機器に関する。

【０００２】

【従来の技術】

確率過程を伴う現象のシミュレーションや各種のセキュリティーのために乱数列を用いる場合、時系列にみた乱数性だけではなく、時系列に並べられた乱数列から同一クロックで取得したデータにおける乱数性も重要である。なぜなら同一クロックで多数データサンプリングすることで、暗号情報を読み取る手口が存在し、その暗号データを乱数と演算処理することで、読み取られにくくする方法に乱数が使われるからである。

【０００３】

擬似乱数生成回路は比較的小型であり、それにより得られた時系列のデータは、比較的高品質な乱数として用いることが可能である。しかし、電源を投入してシステムをオン（ＯＮ）した後に同一クロックで取得したデータを１回目、２回目・・と順番に並べたデータ自体においては、十分な乱数性が保証できない。

【０００４】

図１６は、この事情を説明するための概念図である。すなわち、擬似乱数生成回路を含むシステムをオンにする度に、「０」と「１」とが時系列に出力されて乱数列が生成されるものとする。この時、それぞれの乱数列を時系列（すなわち、同図の横軸方向）にみた場合の乱数性は良好である。しかし、これら乱数列から同一クロックで特定のデータをサンプリングした（同図の縦軸方向にみた）場合、そのデータ系列の乱数性は必ずしも良質とはいえない。例えば、図１６に例示したように、同一クロックデータ列においては、「０」または「１」のいずれ

かの出現頻度が高いというような問題が生ずる。これは、擬似乱数の場合には、擬似乱数回路の「初期値」すなわち「シード」に依存して乱数列が決定されるからである。

【０００５】

図１７は、擬似乱数回路におけるシードの役割を説明するための概念図である。すなわち、同図（ａ）は、擬似乱数回路の一例であるリニア・フィードバック・シフトレジスタを用いた回路を表す。この回路においては、入力されたシードに応じて、データＸが順次出力される。しかし、入力されるシードが固定されていれば、得られる乱数列（同図の横方向の列）も同一である。従って、これら乱数列から同一クロックでサンプリングされて得られる同一クロックデータ列（同図の縦方向の列）は、常に同じデータの配列となってしまう。

【０００６】

仮に、これを「乱す」役割を有する何らかの回路を設けたとしても、同一クロックデータ列は良質の乱数にはなりにくい。すなわち、入力されるシードを毎回、書き換えたとしても、同図（ｃ）に表したように、「０」と「１」とのバランスが１：１からずれたり、何らかの規則性や周期性が存在したりする場合が多い。これは、擬似乱数回路の同一クロックデータ列のランダム性は、入力されるシードのランダム性だけに依存するからである。つまり、擬似乱数回路の場合、入力されるシードのランダム性が極めて重要となる。

【０００７】

起動時に書き換えられるシードが、ソフト的に書き換える場合も多いが、これでシード自身に常に違った乱数性を与えるのはほとんど不可能である。例えば、特許文献１には、「移動体端末の有する機能手段が発生する状態情報のうちで時間的に不規則に変化する再現性のない情報の一部を抽出してサンプルデータとする。サンプルデータをシード１０２として乱数生成部１０３に入力して、乱数１０４を発生する。」方法が開示されている。

【０００８】

【特許文献１】

特開２００２－２１５０３０号公報

【発明が解決しようとする課題】

しかし、特許文献１に開示された技術による場合、サンプルデータ自体にはランダム性はあっても、「０」と「１」のバランスを保つような仕組みや、周期性規則性が存在しないような仕組みが設けられていない。

【０００９】

これに対して、擬似乱数回路においては、シードを常にランダムに書き換える機構が必要である。つまり、ハード的に出現する何らかのランダムネスを利用し、しかも「０」と「１」とのバランスが１：１からずれておらず、規則性や周期性を持たないランダムなシードを作り出す必要がある。

【００１０】

熱雑音等の純粋物理現象で発生するラシダム信号を利用して、乱数を作り、これをシードに利用する手段もあるが、一般的に大型の回路となってしまうため、例えば、半導体集積回路やＩＣカードあるいは各種の情報端末機器などの小型のシステムに内蔵することが困難である。

【００１１】

本発明は、かかる課題の認識に基づいてなされたものであり、その目的は、乱数性の高いシードを生成し、かつ小型の集積回路化が可能なシード生成回路及びこれを用いた乱数生成回路、半導体集積回路、ＩＣカード及び情報端末機器を提供することにある。

【課題を解決するための手段】

上記目的を達成するため、本発明のシード生成回路は、連続的または断続的に発振する発振回路と、前記発振回路から出力されたデジタルデータ列における「０」と「１」との出現頻度を制御して時系列データとして出力する平滑回路と、前記時系列データのうちの複数のビットを用いた演算処理により、１ビットのシードを生成する真性化回路と、を備えたことを特徴とする。

【００１２】

上記構成によれば、乱数性の高いシードを生成し、かつ小型の集積回路化が可能なシード生成回路を実現できる。

【００１３】

ここで、前記発振回路は、入力された複数のデータが特定の組み合わせとなった場合のみ発振するものとすることができる。

【００１４】

またこの場合、前記発振回路は、２つの排他的論理和演算回路と２つの反転回路をそれぞれ交互に直列接続し、前記２つの排他的論理和演算回路のそれぞれの入力の一端に、前記複数のデータのそれぞれを与えるものとしてもよい。

【００１５】

また、前記発振回路は、リング発振回路を含み連続的に発振するものとすることもできる。

【００１６】

一方、前記平滑回路は、擬似乱数を生成する擬似乱数生成手段と、前記発振回路から出力された前記デジタルデータ列と、前記擬似乱数生成手段により生成された前記擬似乱数と、の排他的論理和を演算して前記時系列データとして出力する論理演算手段と、を有するものとすることができる。

【００１７】

また、前記平滑回路は、その出力において、前記発振回路から出力されたデジタルデータ列よりも「０」と「１」との出現頻度が１：１に近いものとすることが望ましい。

【００１８】

一方、前記真性化回路は、前記演算処理を行う排他的論理和演算回路を有するものとすることができる。

【００１９】

また、前記真性化回路は、前記複数のビットの組み合わせに応じて「０」及び「１」のいずれかを割り当てるテーブルに基づいて前記１ビットのシードを生成するものとすることもできる。

【００２０】

一方、本発明の乱数生成回路は、上記いずれかのシード生成回路と、前記シード生成回路により生成された前記シードに基づいて擬似乱数を生成する擬似乱数生成回路と、を備えたことを特徴とする。

【００２１】

上記構成によれば、乱数性の高いシードを生成し、かつ小型の集積回路化が可能な乱数生成回路を実現できる。

【００２２】

ここで、デジタル入力値に対して一義的に決定されないデジタル出力値を与える不確定論理回路をさらに備え、前記擬似乱数を前記不確定論理回路に入力して、その出力を乱数として出力するものとすることができる。

【００２３】

一方、本発明の半導体集積回路は、上記いずれかの乱数生成回路を備えたことを特徴とする。上記構成によれば、乱数性の高いシードを生成し、かつ小型の集積回路化が可能な半導体集積回路を実現できる。

【００２４】

一方、本発明のＩＣＩＣカードは、上記の半導体集積回路を備えたことを特徴とする。上記構成によれば、コンパクトで高いレベルのセキュリティが得られしかも低コストのＩＣカードを実現できる。

【００２５】

一方、本発明の情報端末機器は、上記の半導体集積回路を備えたことを特徴とする。上記構成によれは、上記構成によれば、コンパクトで高いレベルのセキュリティ及び暗号処理技術が得られしかも低コストのＩＣカードを実現できる。

【００２６】

【発明の実施の形態】

以下、図面を参照しつつ、本発明の実施の形態について詳細に説明する。

【００２７】

図１は、本発明の実施の形態にかかるシード生成回路の要部構成を表すブロック図である。すなわち、本実施形態のシード生成回路は、発振回路１０と、平滑回路２０と、を有する。

【００２８】

発振回路１０は、連続的または断続的（非連続的）に発振することによってランダム信号を発生する回路である。ランダム信号を作るのに発振を利用するのは

、小型化が容易だからである。一方、平滑回路２０は、発振回路１０から出力されたランダム信号の「０」と「１」とのバランスをとり、かつその周期性や規則性を壊す回路である。このような構成により、「０」と「１」とのバランスを時系列的に一様にすることができる。さらに、時系列的に生成した多数ビットを使って、所定の演算処理により、１ビットのランダムな擬似乱数用のシードを生成することができる。

【００２９】

図２は、発振回路１０の具体例を表す模式図である。すなわち、本具体例の発振回路は、２つの入力Ｘ１、Ｘ２に対して、２つの出力Ｑ１、Ｑ２を与える。２つの入力Ｘ１、Ｘ２の値が同じ場合には、偶数インバータを備えたフリップフロップと等価の動作をする。一方、２つの入力Ｘ１、Ｘ２が異なる場合には、リング発振する回路である。従って、２つの入力Ｘ１、Ｘ２の値が同じ場合と異なる場合との割合が半々であれば、回路動作期間の半分の期間だけ発振する。

【００３０】

またさらに、図２の回路は、単純な発振回路とは異なり、初期値Ｚの値によっても出力が異なる。すなわち、初期値Ｚが「１」の場合には、入力Ｘ１、Ｘ２がいずれも「１」の時には出力Ｑ１、Ｑ２はいずれも「０」となり、入力Ｘ１、Ｘ２がいずれも「０」の時には出力Ｑ１は「１」、Ｑ２は「０」となる。

【００３１】

一方、初期値Ｚが「０」の場合には、入力Ｘ１、Ｘ２がいずれも「１」の時には出力Ｑ１、Ｑ２はいずれも「１」となり、入力Ｘ１、Ｘ２がいずれも「０」の時には出力Ｑ１は「０」、Ｑ２は「１」となる。

【００３２】

このように、図２の具体例の発振回路１０は、２つの入力Ｘ１、Ｘ２が異なる場合にのみ発振する点で、「断続的発振回路」であるといえる。連続的発振回路は、乱数データに周期性が残りやすいという点と、消費電流が大きいという点が弱点であり、断続的発振回路は、この点を改善した回路である。

【００３３】

一方、図３は、発振回路１０のもう一つの具体例を表す模式図である。すなわ

ち、本具体例の発振回路は、３つのインバータを直列接続したリング発振器であり、「連続的発振回路」であるといえる。この場合、発振周波数は、概ねシステムクロックの１０倍以上であることが望ましい。

【００３４】

次に、本発明における平滑回路２０について説明する。

【００３５】

図４は、本発明における平滑回路２０の基本的な構成を表すブロック図である。すなわち、平滑回路２０は、擬似乱数出力手段２０Ａと、ＸＯＲ（排他的論理和）演算手段２０Ｂとを有する。擬似乱数出力手段２０Ａとしては、例えば、リニア・フィードバック・シフト・レジスタ（Linear Feedback Shift Resistor：ＬＦＳＲ）などを用いることができる。

【００３６】

このようにして、発振回路１０から得られたランダム信号と、擬似乱数出力とのＸＯＲ（排他的論理和）を取ることにより、ランダム信号の一様性を著しく改善することができる。ただしこの場合、発振回路１０と擬似乱数出力２０Ａとの出力の間に相関性がないことが望ましい。以下、この点について詳述する。

【００３７】

まず、独立した２つの回路からの出力をＱ１、Ｑ２とする。Ｑ１、Ｑ２には相関が無いとする。このとき、Ｑ１における「１」の出現比率をｐ、Ｑ２における「１」の出現比率をｑとする。すると、Ｑ１とＱ２とをＸＯＲした出力Ｒが「１」となる出現比率ｒは、以下の式で与えられる。

【００３８】

$$r = p + q - 2pq \qquad (1)$$

ＸＯＲ出力における「１」と「０」との出現比率の差は、次式により与えられる。

【００３９】

｜ｒ－（１－ｒ）｜＝｜（１－２ｐ）（１－２ｑ）｜　　（２）

Ｑ１とＱ２の出力における「１」と「０」の出現比率の差は、それぞれ、｜１－２ｐ｜、｜１－２ｑ｜であり、ｐとｑはともに、０以上１以下なので、次式が得られる。

【００４０】

｜（１－２ｐ）（１－２ｑ）｜＜｜１－２ｐ｜，｜１－２ｑ｜　（３）

これは、ＸＯＲする前よりも、ＸＯＲした後のほうが、「０」と「１」の出現比率の差が小さくなること、つまり「偏り」が小さくなることを表している。従って、複数個のデータを並列化してＸＯＲしていくと、単独の出力よりも「偏り」が小さくなる。例えば、出力が偏った回路が多数あっても、出力の「偏り」の小さいものが一つでも存在すれば、その一つの回路出力よりもさらに「偏り」が小さい出力が得られることになる。

【００４１】

一方、相関がある場合には、次のようになる。すなわち、独立した２つの回路からの出力をＱ１、Ｑ２とする。Ｑ１、Ｑ２には何らかの理由で相関があるとする。このとき、Ｑ１の１の出現比率をｐ、Ｑ２のそれをｑとする。Ｑ１とＱ２に相関がある場合には、Ｑ１が「１」の場合に、Ｑ２が「１」となる確率は、単純にｑではなく、ϕの割合だけずれるとする。ϕが「１」からずれている度合いが相関性を表す。

【００４２】

そうすると、出現確率は以下の如くとなる。

【００４３】

Ｑ１が「１」の場合に、Ｑ２が「１」となる確率＝ｐｑϕ

Ｑ１が「１」の場合に、Ｑ２が「０」となる確率＝（１－ｑ）ϕｐ

Ｑ１が「０」の場合に、Ｑ２が「１」となる確率＝ｑ（１－ϕｐ）

Ｑ１が「０」の場合に、Ｑ２が「０」となる確率＝（１－ｑ）（１－ϕｐ）

【００４４】

Ｑ１とＱ２とをＸＯＲした出力Ｒについて、「１」（Ｑ１とＱ２が等しくない）の出現比率ｒは、次式により与えられる。

【００４５】

$$r=(1-q)\phi p+q(1-\phi) \qquad (4)$$

出力Ｒにおける「１」と「０」の出現比率の差は、次式により得られる。

【００４６】

$$|r-(1-r)|=|1-2\phi p||1-2q| \qquad (5)$$

つまり、相関がある場合、Ｑ１とＱ２のＸＯＲ＝Ｒでは、Ｑ１、Ｑ２の１の出現確率は、ｐとｑだけでなく、相関の度合いϕにも影響を受ける。そして、ｐとｑがそれぞれ「０．５」に近い値の場合は、次式により表される。

【００４７】

$$|r-(1-r)|=|1-\phi| \qquad (6)$$

ここで相関性が無い場合はϕが「１」となり、「０」と「１」は均一となる。逆に、相関が強くϕが「０」または「２」程度になると、Ｒはほとんど全て「１」または「０」となってしまう。

【００４８】

従って、平滑回路２０においてＸＯＲを演算する場合には、その２つの入力Ｑ１とＱ２に相関性を持たせないようにする工夫が必要である。つまり、発振回路１０と擬似乱数出力手段２０Ａとの間に相関性が生じないようにすることが望ましい。

【００４９】

例えば、これら２つの回路に、同じクロックをダイレクトに入力しないことが

望ましい。アナログ的な動作をする回路の場合には、Ｑ１とＱ２の出力端も別個にラッチすることが望ましい。発振回路１０と擬似乱数出力手段２０Ａは、これらの点に気をつけて設計する必要がある。

【００５０】

以上、平滑回路２０が有する、一様化の作用について詳述した。

【００５１】

一方、平滑回路２０は、同一クロックデータ列における周期性を乱す作用も有する。すなわち、出力を時系列に並べると、ＦＩＰＳ１４０－２検定を通る乱数があるとする。しかし、このような乱数をもとにして、ある時間で発生した１ビットを単純にシードにするだけでは、同一クロックでのランダムネスが十分に得られない。そこで、本発明においては、時系列的に生成した多数ビットを使って１ビットの乱数データを作る。その典型的なものは、複数データの全てにＸＯＲを取ることである。つまり、時系列データをＸ１，Ｘ２，Ｘ３・・・Ｘｎとした場合、次式により、ｎ個の時系列データから１ビットの乱数データを作る。

【００５２】

【数１】

$$W_1 = X_1 \oplus X_2 \oplus X_3 \oplus \cdots \oplus X_n \qquad (7)$$

これは、一様性に関して前述したものと同様の効果によって、「０」と「１」との出現確率の均一性（一様性）を向上する方法である。これは時系列での効果であるが、複数の時系列データから同一クロックでサンプリングして得られた同一クロックデータ列における乱数性を上げる効果もあることが分かる。この点について、以下に説明する。

【００５３】

すなわち、前述したように、シードが固定である場合、ＬＦＳＲの出力データにおいては、同一クロックでは常に同じデータが並ぶ。時系列データがＸ１，Ｘ２，Ｘ３・・・Ｘｎの場合、同一クロックのデータに関する予測確率をそれぞれｆ１，ｆ２，ｆ３・・・ｆｎとする。ここで予測確率は、「０」と「１」の出現

確率をそれぞれ（０．５＋ｆｋ），（０．５－ｆｋ）と定義することにする。ＬＦＳＲの場合、全て予測可能なので、次式が与えられる。

【００５４】

$$fk = \pm 0.5 \quad (k = 1, 2 \cdots n) \qquad (8)$$

同一クロック配列が乱数性を持つことは、ｆｋが「０」に近づくこと、つまり予測困難であることを意味する。

【００５５】

いま、クロックの異なる二つの出力Ｘｊ，Ｘｈを選び、このＸＯＲをＸｊｈとする。

【００５６】

【数２】

$$Xjh = X_j \oplus X_h$$

例えば、Ｘｊの予測確率が「０．４」、Ｘｈの予測確率が「０．３」である場合を考える。Ｘｊｈが「１」となるのは、Ｘｊ＝１、Ｘｈ＝１またはＸｊ＝０，Ｘｈ＝１の場合である。従って、その確率は、０．９×（１－０．８）＋（１－０．９）×０．８＝０．２６であり、予測確率ｆｊｈは「０．２４」である。つまり、ＸｊとＸｈの排他的論理和（ＸＯＲ）の予測確率ｆｊｈは、Ｘｊ、Ｘｈの予測確率ｆｊ，ｆｈよりも小さい。つまり、排他的論理和をとることによって、予測困難性が上がっていることが分かる。これを一般的に表すと、ＸｊとＸｈ排他的論理和Ｘｊｈの予測確率ｆｊｈは、次式の如くとなる。

【００５７】

$$fjh = 0.5-(0.5+fj)(0.5-fh)-(0.5-fj)(0.5+fh)$$
$$= 2fj \times fh \qquad (9)$$

ｆｊ，ｆｈは、共に絶対値が「０．５」よりも小さいので、ＸｊとＸｈの排他的論理和Ｘｊｈの予測確率ｆｊｈはＸｊ，　Ｘｈの予測確率ｆｊ，ｆｈよりも小さいことが一般的に証明できる。従って、排他的論理和をとる時系列のデータ数を重ねていくほど、同一クロックにおけるデータ列の予測確率が小さくなっていく。その結果として、複数の時系列データから同一クロックでサンプリングした同一クロックデータ列における周期性を低下させ、良質のシードを与えることができる。

【００５８】

以上、平滑回路２０について説明した。

次に、真性化回路３０について説明する。

【００５９】

図５は、真性化回路３０の作用を説明するための模式図である。すなわち、真性化回路３０は、平滑回路２０から出力された乱数列を演算処理し、１ビットのシードを生成する。その具体的な構成については、以下に具体例を参照しつつ説明する。

【００６０】

（第１の具体例）

図６は、本発明の第１の具体例にかかるシード生成回路を表すブロック図である。すなわち、このシード生成回路は、図２に表した発振回路１０を備えている。前述したように、この発振回路１０は、「断続的発振回路」であり、２つの入力Ｘ１、Ｘ２が異なる場合のみ、リング発振する。そして、これら２つの入力Ｘ１、Ｘ２の値が同じ場合と異なる場合が半々であれば、回路動作時の半分の時間だけ発振する。

【００６１】

一方、平滑回路２０は、擬似乱数出力手段２０Ａとして、１３段のシフトレジスタを有するＬＦＳＲを設けることができる。そして、発振回路１０とＬＦＳＲの出力とを平滑回路２０においてＸＯＲを演算することにより、例示したような乱数列が得られる。

【００６２】

一方、真性化回路３０は、このように時系列的に生成される多数ビットのＸＯＲを演算することにより、１ビットのシードを生成する。この回路をｎクロック分だけ動作させると、ｎビットの時系列データのＸＯＲがＱに出力される。

【００６３】

本具体例のシード生成回路の場合、必要な論理ゲート数は、周辺回路を含めても約５０ゲート程度であり、回路規模は小さい。入力Ｘ１として、ロー（Ｌｏｗ）レベルかハイ（Ｈｉｇｈ）レベルに固定した値を入力し、Ｘ２としては基準クロックを入力する。これにより、発振（不確定出力）と確定出力とを交互に繰り返す動作が実行される。この場合、クロックは、他の回路用のクロックと同期していても良く、または非同期でも良い。

【００６４】

本具体例のシード生成回路を作製して６４クロック分の時系列データのＸＯＲ出力を２００００個（同一クロックデータ列）取得して、これを統計的な検定にかけた。図７は、この結果を表す一覧表である。すなわち、同図には、技術標準局（ＮＩＳＴ）による検定規格ＦＩＰＳ１４０－２と、棄却率５％の一般検定の結果を表した。また、図７には、比較例として、熱雑音増幅型の物理乱数回路を用いた場合の結果と、１６段のＬＦＳＲから得られた結果も表した。

【００６５】

図７から分かるように、本具体例のシード生成回路によれば、同一クロックの１ビットのシード列（同一クロックデータ列）においても、ＦＩＰＳ１４０－２の検定だけでなく、棄却率５％の難解な一般検定もクリアする良好な乱数性が得られることが確認された。物理乱数回路の場合、時系列データと同一クロックデータ列とは基本的に同一である。一方、ＬＦＳＲの場合は、シードが固定されているので同一クロックデータ列においてはいつも同じデータが並ぶため、当然ながら全ての検定は不合格となる。

【００６６】

図８は、８個のシード生成回路について、システム起動後のクロック数と乱数データの各１ビットについて、一様性の改善の傾向を表すグラフ図である。同図から、クロック数が増すほど一様性が改善されることが確認された。なお、発振

回路１０は消費電流が比較的大きいので、ある程度のランダム性をもつ出力データが得られたら、そのデータを平滑回路２０に受け渡し、発振回路１０は停止させればよい。

【００６７】

（第２の具体例）

図９は、本発明の第２の具体例にかかるシード生成回路を表す模式図である。本具体例においては、発振回路１０として、図３に表したリング発振器を用いている。つまり、本具体例は、「連続的発振回路」を用いたシード生成回路であるといえる。この場合、発振回路の発振周波数は、概ねシステムクロックの１０倍以上が望ましい。前述したように、発振回路１０のリング発振回路は、他の回路と非同期とすることが望ましい。

【００６８】

一方、平滑回路２０は、擬似乱数生成回路２０Ａと、ＸＯＲ演算手段２０Ｂと、を有する。擬似乱数生成回路２０Ａは、１１段のシフトレジスタからなるＬＦＳＲの最下位２ビットの論理積（ＡＮＤ）と、次位の１ビットの反転との論理和（ＯＲ）をとって、最上位の１ビットとＸＯＲしたものを最下位のシフトレジスタに戻す回路であり、非線形の擬似乱数生成回路であるといえる。

【００６９】

リング発振器の出力と、擬似乱数生成回路２０Ａの出力と、をＸＯＲ演算手段２０Ｂにおいて演算し、時系列に発生するランダムデータ列を得る。

【００７０】

このランダムデータ列は、真性化回路３０において処理され、１ビットのシードが得られる。真性化回路３０においては、図示したように、データ列のうちで続いた２ビットが「０１」または「１０」というように、違った数字が並ぶ場合には、「１」に変換し、一方、続いた２ビットが「１１」または「００」というふうに、同じ数字が並ぶ場合には、「０」に変換する処理を実行する。これを１ビットになるまで繰り返し、１ビットのシードを生成する。

【００７１】

（第３の具体例）

次に、本発明の第３の具体例として、真性化回路３０における処理の変型例を説明する。

【００７２】

図１０は、本具体例にかかるシード生成回路を表す模式図である。本具体例の場合、平滑回路２０において、４の倍数すなわち４ｎ個の時系列データを生成させておく（ｎは任意の数）。この時系列データを真性化回路３０において４個のデータの組み合わせ毎にそれぞれ図示したように分類して、「０」または「１」に変換する。これをｎ回繰り返して１ビットを作る。

【００７３】

このように、ｎビットを１ビットに変換するテーブル（変換表）を用意しておき、このテーブルに対応する変換を実行するための変換回路を論理回路で作製すれば真性化回路３０が得られる。このとき、テーブルは、「０」と「１」とが等しい確率で変換されるように作られなければならない。それが満たされていれば、どんなテーブルでも良い。

【００７４】

（第４の具体例）

次に、本発明の第４の具体例として、本発明のシード生成回路を備えた乱数生成回路について説明する。

【００７５】

図１１は、本具体例にかかる乱数生成回路を表す模式図である。すなわち、この乱数生成回路１００は、シード生成回路１１０と、擬似乱数生成回路１２０と、不確定論理回路１３０と、を有する。

【００７６】

シード生成回路１１０は、図１乃至図１０に関して前述したような本発明のシード生成回路である。擬似乱数生成回路１２０は、例えば、ＬＦＳＲなどを用いて擬似乱数を生成する回路である。

【００７７】

一方、不確定論理回路１３０としては、本発明者が特願２００２－１８３９６７号において開示した不確定論理回路を用いることかできる。この回路は、デジ

タル入力値に対して一義的に決定されないデジタル出力値を与える。すなわち、特定の入力信号の組み合わせに対して出力の「０」または「１」が不確定になる作用を有する。論理出力が不確定の場合、不確定論理回路１０を構成する素子のその時々の物理的な要因によって、出力が変動する。この物理現象を利用することにより、一定の入力に対して、出力が変動する（不確定となる）デジタル回路が得られ、「０」と「１」とのランダムなデジタル信号列が得られる。

【００７８】

本具体例の乱数生成回路１００の場合、シード生成回路１１０により生成されたシードが擬似乱数生成回路１２０に入力されて擬似乱数が生成される。そして、擬似乱数生成回路１２０が持っている周期性を不確定論理回路１３０により壊す。この結果、得られる乱数の質がより高品質になる。不確定論理回路１３０を合体すると回路規模自体は凡そ２倍になるが、それでもせいぜい１０００ゲート程度であるので、後に詳述するように、ＩＣ（半導体集積回路）、ＩＣカード用チップ、小型携帯端末などに搭載可能である。

【００７９】

（第５の具体例）

次に、本発明の第５の具体例として、本発明のシード生成回路を設けた半導体集積回路（ＩＣ）について説明する。

【００８０】

図１２は、本具体例の半導体集積回路の要部構成を表す模式図である。本具体例は、例えばＩＣカードなどに搭載することができるＩＣであり、演算部（ＭＰＵ）、メモリ（ＲＡＭ，ＲＯＭ，ＥＥＰＲＯＭ）、補助演算部（Co-processor）、乱数生成回路１００を有する。ここで、補助演算部（Co-processor）は、暗号処理を実行する役割を有する。

【００８１】

乱数生成回路１００において、本発明のシード生成回路と、例えば通常の擬似乱数生成回路などを組み合わせることにより、高品質の乱数を生成させることができる。この乱数生成回路１００を搭載することで、演算部（ＭＰＵ）や暗号処理専用の補助演算部（Co-processor）が常に高品質の乱数を読み出して使うこと

ができ、また、暗号鍵をＩＣの消費電流信号から読み出すハッキング技術に対する対策として、乱数を使って消費電流の変化を撹乱させることにも使え、高度な暗号セキュリティが実現可能となる。

図１３は、本具体例の半導体集積回路２００の回路規模を説明するための概念図である。すなわち、本発明のシード生成回路と、通常の擬似乱数生成回路などとを組み合わせた乱数生成回路１００、全てＣＭＯＳ論理回路のみで構成できる。しかも論理ゲートの数は、わずか数１００程度で済むので、各種のＩＣに搭載可能である。その回路規模は、図１３に例示した程度あるいはそれ以下であり、ＩＣ全体のサイズを大幅に増大させるという問題も生じない。

【００８２】

本発明の乱数生成回路を搭載することで、高度な暗号セキュリティ機能が利用可能になる。またゲーム機やモンテカルロシュミレーション用の乱数にも用いることができる。

【００８３】

（第６の具体例）

次に、本発明の第６の具体例として、本発明の乱数生成回路を搭載したＩＣカード及び携帯型の情報端末機器について説明する。

【００８４】

図１４は、本具体例のＩＣカード及び情報端末機器を表す模式図である。すわなち、同図において３００は、本具体例のＩＣカードまたは情報端末機器を表す。ＩＣカードとしては、例えば、銀行の預金カードや各種のプリペイドカード、企業などにおける社員証、入門セキュリティカードなどを挙げることができる。また、情報端末器器としては、例えば、携帯電話や、その他の携帯型端末を挙げることができる。このような携帯型端末は、例えば、、ワードプロセッサ、表計算、スケジューラ、ゲーム、電子メールの送受信、静止画や動画の撮影、などの各種の機能のうちのいずれかを備えたものを挙げることができる。

【００８５】

例えば、図１５に表したような携帯電話３００においても、本発明の乱数生成回路１００を搭載することができる。またこれと類似した携帯型情報端末におい

ても同様である。

【００８６】

そして、本発明においては、シード生成回路と、通常の擬似乱数生成回路などとを組み合わせた乱数生成回路１００を搭載することにより、非常に小型で消費電力も抑制しつつ高度な暗号セキュリティ機能を付加することができる。すなわち、乱数生成回路１００を用いることにより、例えば、使用者の認証プロセスや、取り扱うデータの暗号化とその復元などをはじめとして、ゲーム機能に利用したり、モンテカルロシュミレーション用の乱数にも用いることができる。

以上、具体例を例示しつつ本発明の実施の形態について説明した。しかし、本発明は、上述した各具体例に限定されるものではない。

【００８７】

例えば、本発明において用いる発振回路、平滑回路、真性化回路、擬似乱数生成回路及び不確定論理回路の具体的な構成に関しては、上記の具体例に限定されず、その機能あるいは作用が同様な全ての回路に置換したものも本発明の範囲に包含される。

【００８８】

例えば、出力が不確定なフリップフロップを複数個、並列もしくは直列に並べた論理回路を擬似乱数生成回路として用いることもできる。

【００８９】

また、本発明の乱数生成回路によって作られたデジタル乱数は、そのまま使用することもできるが、これをフィードバックシフトレジスタのシードとして用いることにより、新たな乱数を生成することもできる。

【００９０】

【発明の効果】

以上詳述したように、本発明によれば、シード生成回路により、同一クロックデータ列に乱数性を持たせることが可能となり、これをシードに利用することで、同一クロックのデータ列においても高い乱数性を得ることができる。

【００９１】

連続発信する発信回路、平滑回路、ならびに真性化回路の各単位回路ブロック

を例えば図１の如く組み合わせることにより、同一クロックのデータ列が高い乱数性を持つことは、本発明以前には知られていなかった効果である。

【００９２】

しかも、本発明によれば、このような高品質の乱数を、フリップフロップ型の論理回路などを利用することにより少ない論理ゲート数で構成できるので、小規模な回路で済む。

【００９３】

すなわち、本発明によれば、真性度が高い乱数をコンパクト、低消費電力且つ低価格で実現できるようになり、例えばＩＣカードや情報端末機器などに応用してセキュリティーの確実な安価なシステムを実現できる点で産業上のメリットは多大である。

【図面の簡単な説明】

【図１】

本発明の実施の形態にかかるシード生成回路の要部構成を表すブロック図である。

【図２】

発振回路１０の具体例を表す模式図である。

【図３】

発振回路１０のもう一つの具体例を表す模式図である。

【図４】

本発明における平滑回路２０の基本的な構成を表すブロック図である。

【図５】

真性化回路３０の作用を説明するための模式図である。

【図６】

本発明の第１の具体例にかかるシード生成回路を表すブロック図である。

【図７】

第１具体例のシード生成回路を統計的な検定にかけた結果を表す一覧表である。

【図８】

８個のシード生成回路について、システム起動後のクロック数と乱数データの各１ビットについて、一様性の改善の傾向を表すグラフ図である。

【図９】

本発明の第２の具体例にかかるシード生成回路を表す模式図である。

【図１０】

本発明の具体例にかかるシード生成回路を表す模式図である。

【図１１】

本発明の具体例にかかる乱数生成回路を表す模式図である。

【図１２】

本発明の具体例の半導体集積回路の要部構成を表す模式図である。

【図１３】

本発明の具体例の半導体集積回路２００の回路規模を説明するための概念図である。

【図１４】

本発明の具体例の情報端末機器を表す模式図である。

【図１５】

本発明の情報端末機器としての携帯型電話である。

【図１６】

同一クロックデータ列における乱数性を説明するための概念図である。

【図１７】

擬似乱数回路におけるシードの役割を説明するための概念図である。

【符号の説明】

１００　乱数生成回路

１１０　シード生成回路

１２０　擬似乱数生成回路

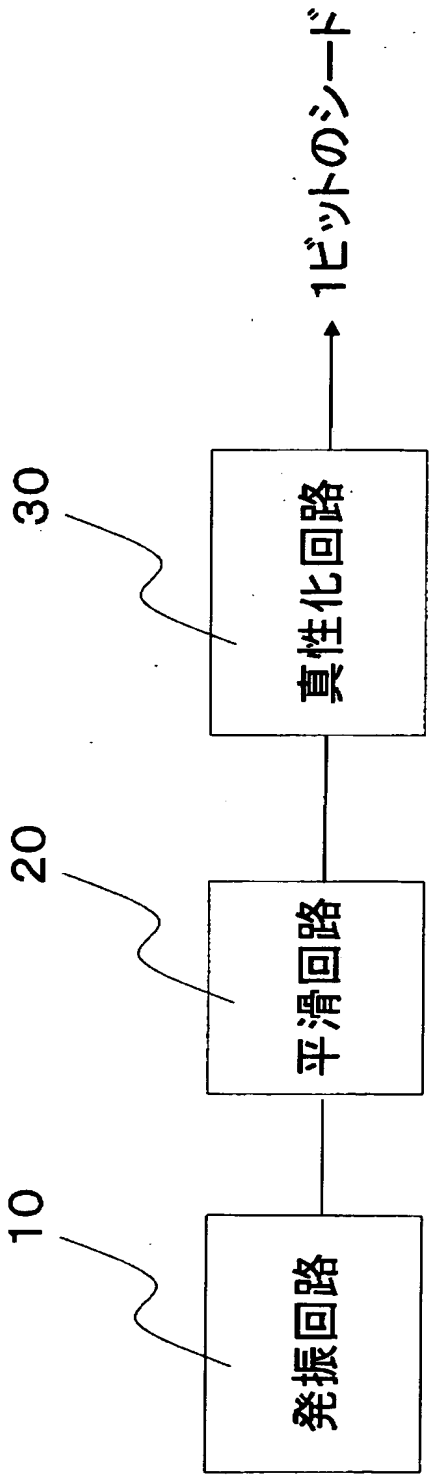
１３０　不確定論理回路

２００　半導体集積回路

３００　ＩＣカード及び情報端末機器

【書類名】　図面

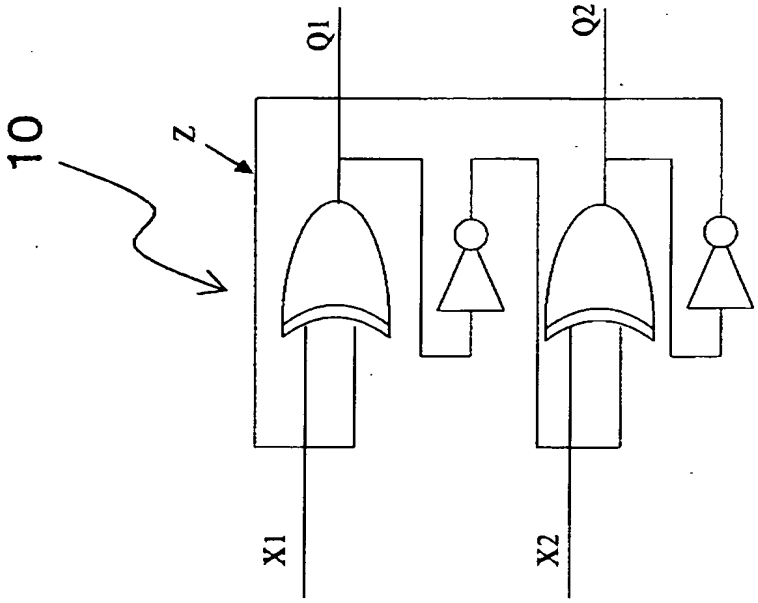
【図１】



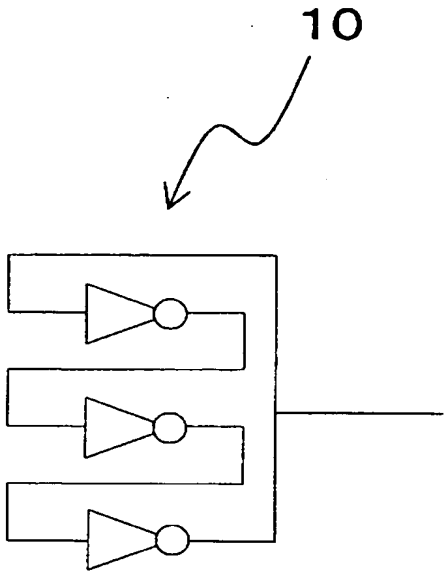
【図２】

If X1 = X2,
フリップフロップ（インバータが偶数個）と等価
Z=1のとき
・X1 = X2= 1 ならばQ1=0, Q2=0
・X1 = X2=0 ならばQ1=1, Q2=0
Z=0のとき
・X1 = X2= 1 ならばQ1=1, Q2=1
・X1 = X2=0 ならばQ1=0, Q2=1

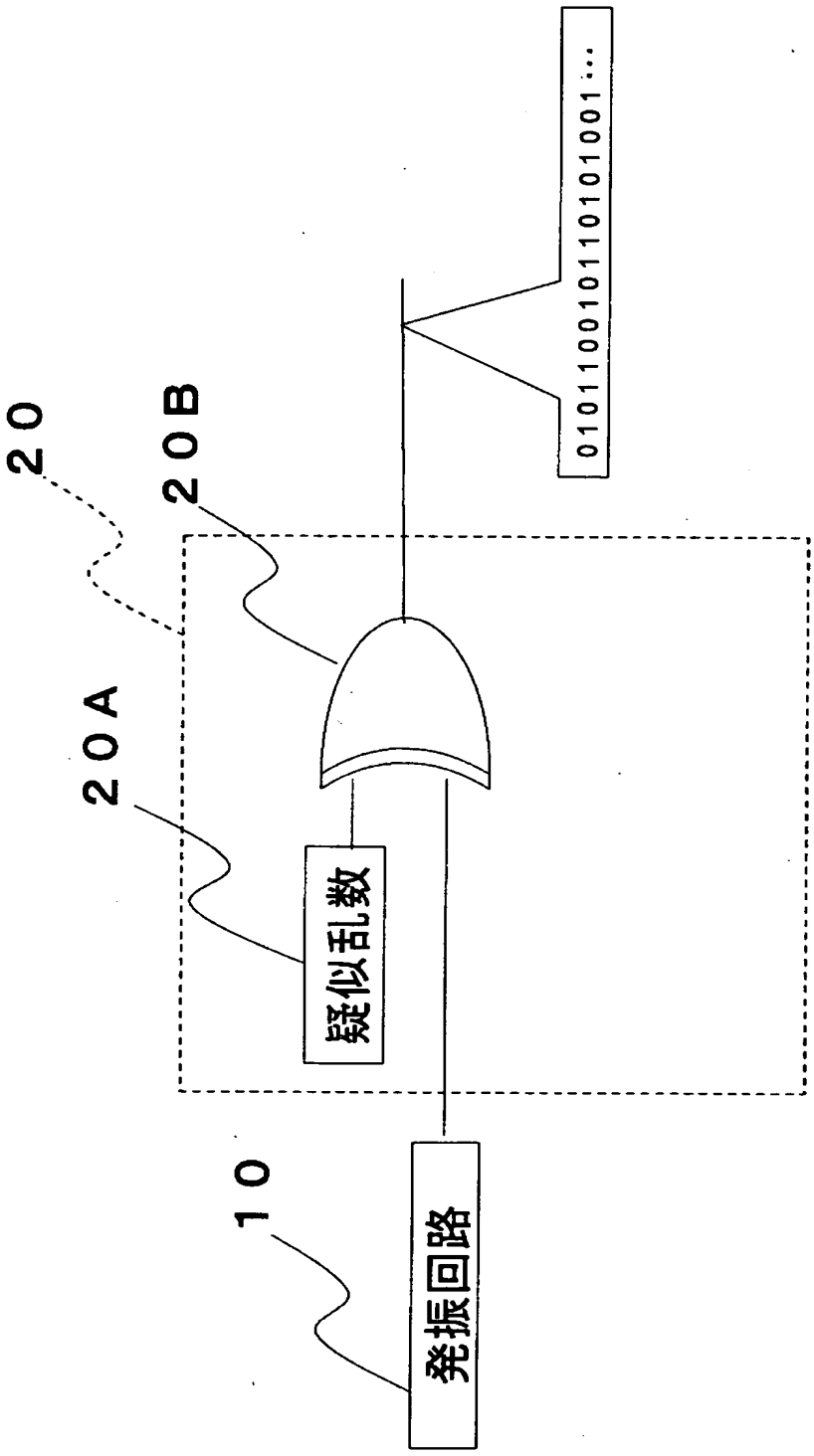
If X1≠X2,
リング発振器と等価



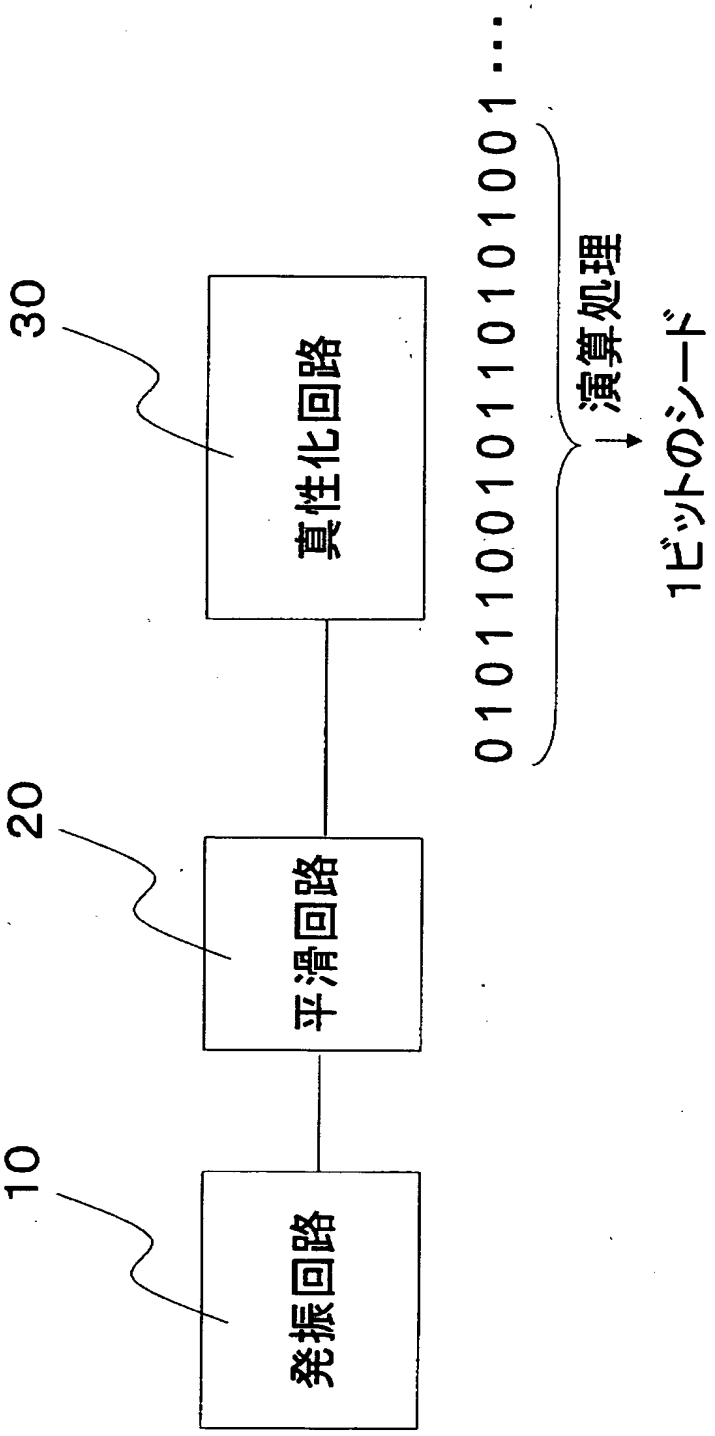
【図３】



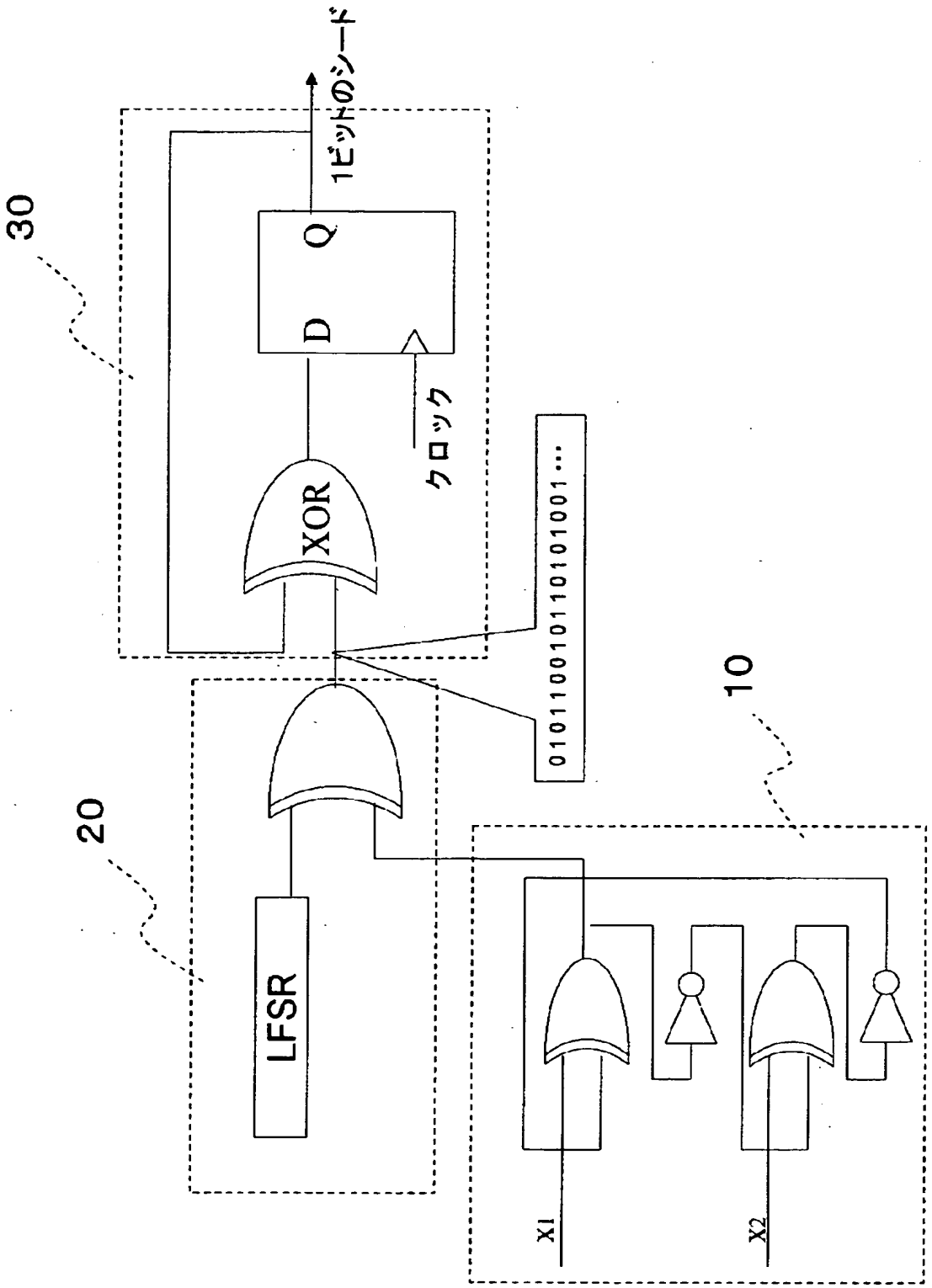
【図４】



【図５】


10
発振回路
20
平滑回路
30
真性化回路
0101100101101101001…
演算処理
1ビットのシード

【図６】

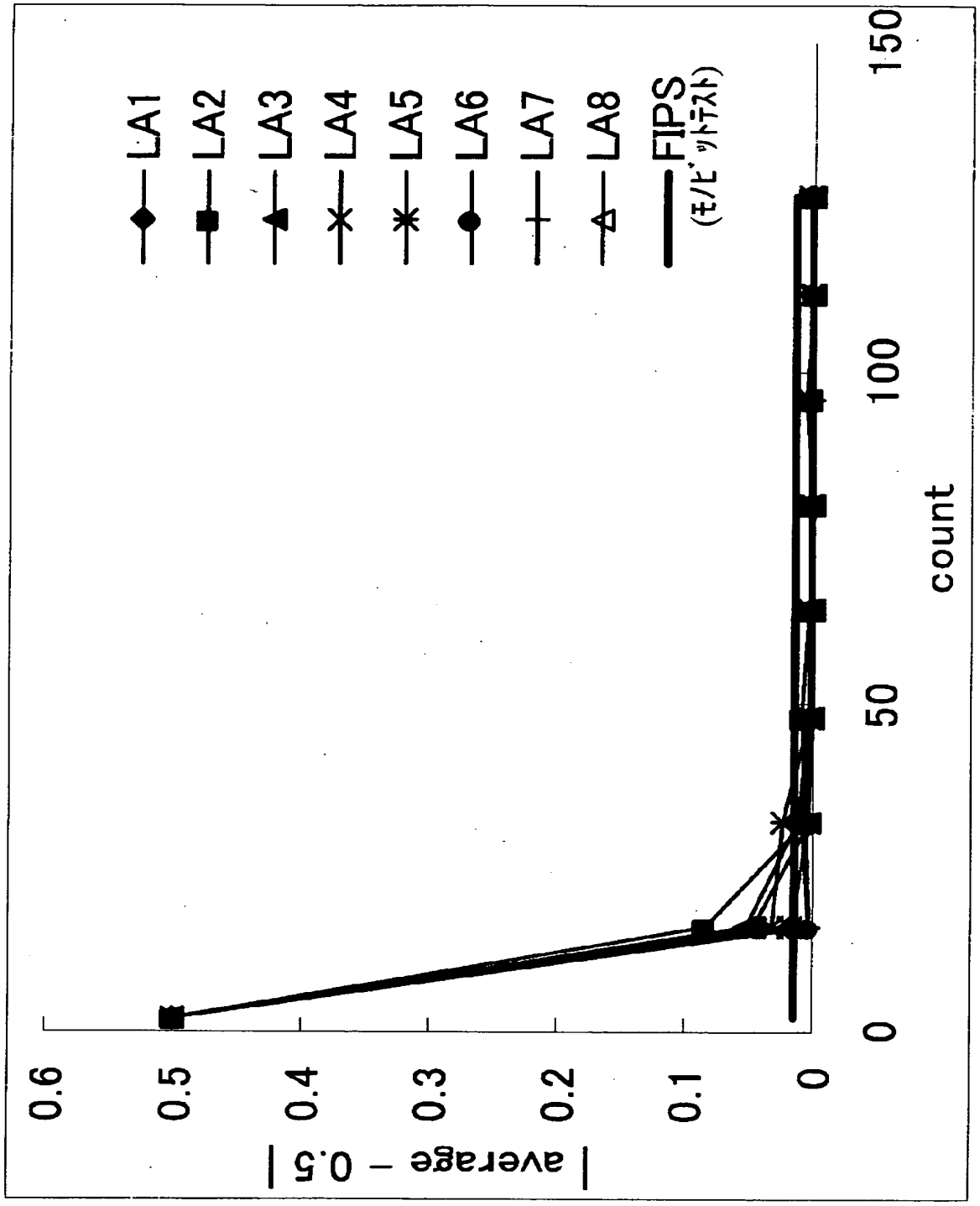

30
1ビットのシード
Q
D
クロック
XOR
0101100101101010011…
10
20
LFSR
X1
X2

【図７】

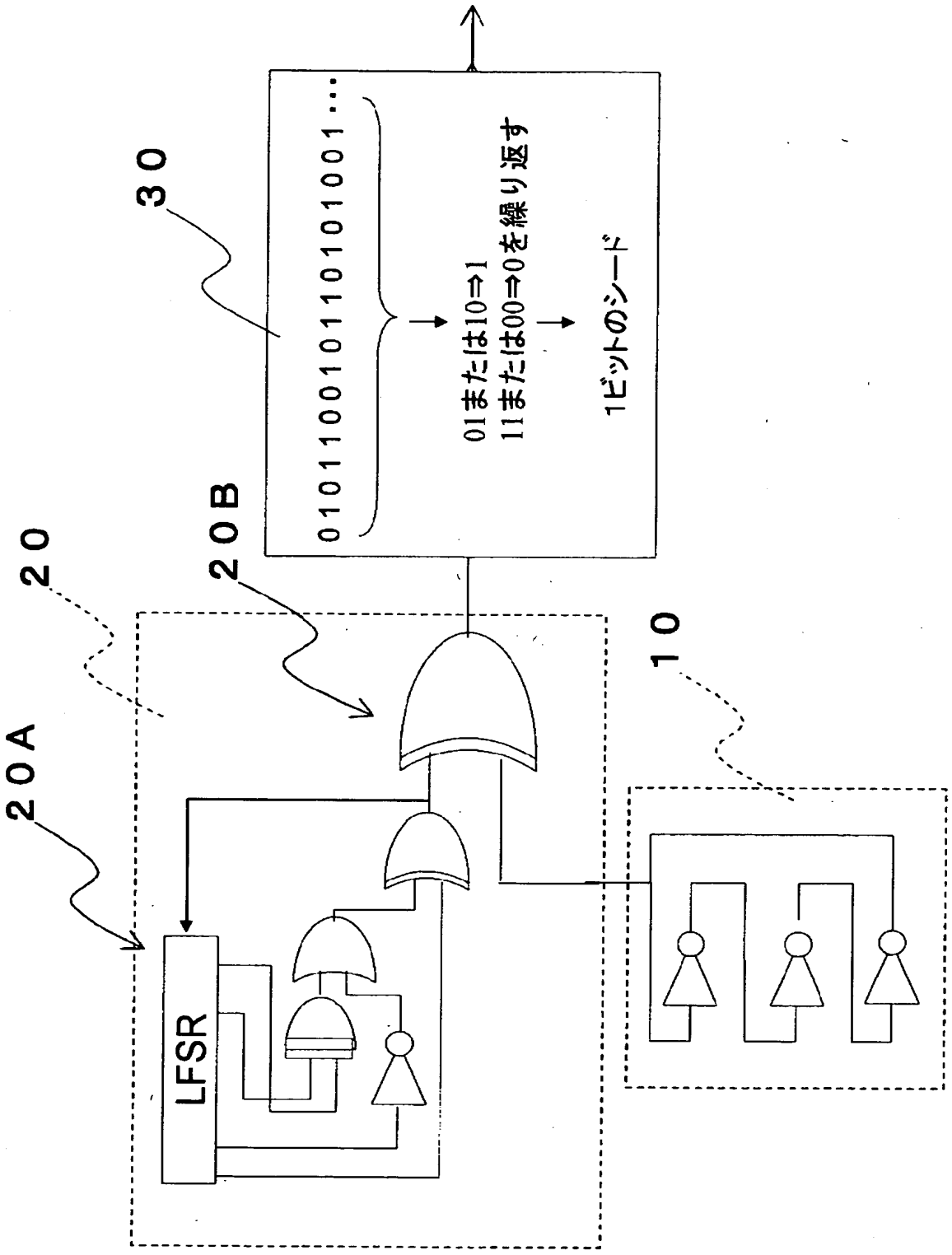
<FIPS140-2>	20000data	熱雑音増幅型		擬似乱数(16段LFSR)		本提案	
Monobit	9725 ~ 10275: 10000±275	10059	◎		×	10221	○
Run1	2315 ~ 2685: 2500±185	2588 2564	◎		×	2584, 2498	◎
Run2	1114 ~ 1368: 1241±127	1282 1246	◎		×	1284, 1264	◎
Run3	527 ~ 723: 625±98	610, 650	◎		×	593, 595	◎
Run4	240 ~ 384: 312±72	302, 327	◎		×	316, 349	◎
Run5	103 ~ 209: 156±53	148, 139	◎		×	145, 176	◎
Runover6	103 ~ 209: 156±53	144, 148	◎		×	120, 160	◎
Poker test	2.16<X<46.17: 24.165±22.005	10.22	◎		×	20.6336	◎
long run	longest run < 26				×	14, 17	◎
					×		
<General test>	8000data				×		
χ２乗検定	QK >0.05	0.14	△		×	0.202465	○
Run test	Pv >0.01	0.153	○		×	0.543148	◎
Freq. Test in bloc	QK >0.05	0.745	◎		×	0.217996	◎
Poker Test	QK >0.05	0.272	◎		×	0.510356	◎
Serial Cor. Test	-0.022491<C<0.02241	-0.0163	△		×	-0.007205	◎
Gap test:0	QK >0.05	0.901896	◎		×	0.664227	◎
Gap test:1	QK >0.05	0.19484	◎		×	0.591764	◎
Gap test:2	QK >0.05	0.56847	◎		×	0.849706	◎
Gap test:3	QK >0.05	0.89883	◎		×	0.017445	◎
Gap test:4	QK >0.05	0.849298	◎		×	0.220639	◎
Gap test:5	QK >0.05	0.615556	◎		×	0.315313	◎
Gap test:6	QK >0.05	0.333719	◎		×	0.004307	◎
Gap test:7	QK >0.05	0.629796	◎		×	0.466615	◎
Gap test:8	QK >0.05	0.281213	◎		×	0.218405	◎
Gap test:9	QK >0.05	0.879929	◎		×	0.072952	○
Gap test:10	QK >0.05	0.339877	◎		×	0.656671	◎
Gap test:11	QK >0.05	0.57006	◎		×	0.633447	◎
Gap test:12	QK >0.05	0.112747	◎		×	0.743529	◎
Gap test:13	QK >0.05	0.885725	◎		×	0.787189	◎
Gap test:14	QK >0.05	0.080402	○		×	0.485003	◎
Gap test:15	QK >0.05	0.747962	◎		×	0.931562	◎

◎余裕もって合格(QK>0.1)　○合格　△▲ボーダーで合否　×失格

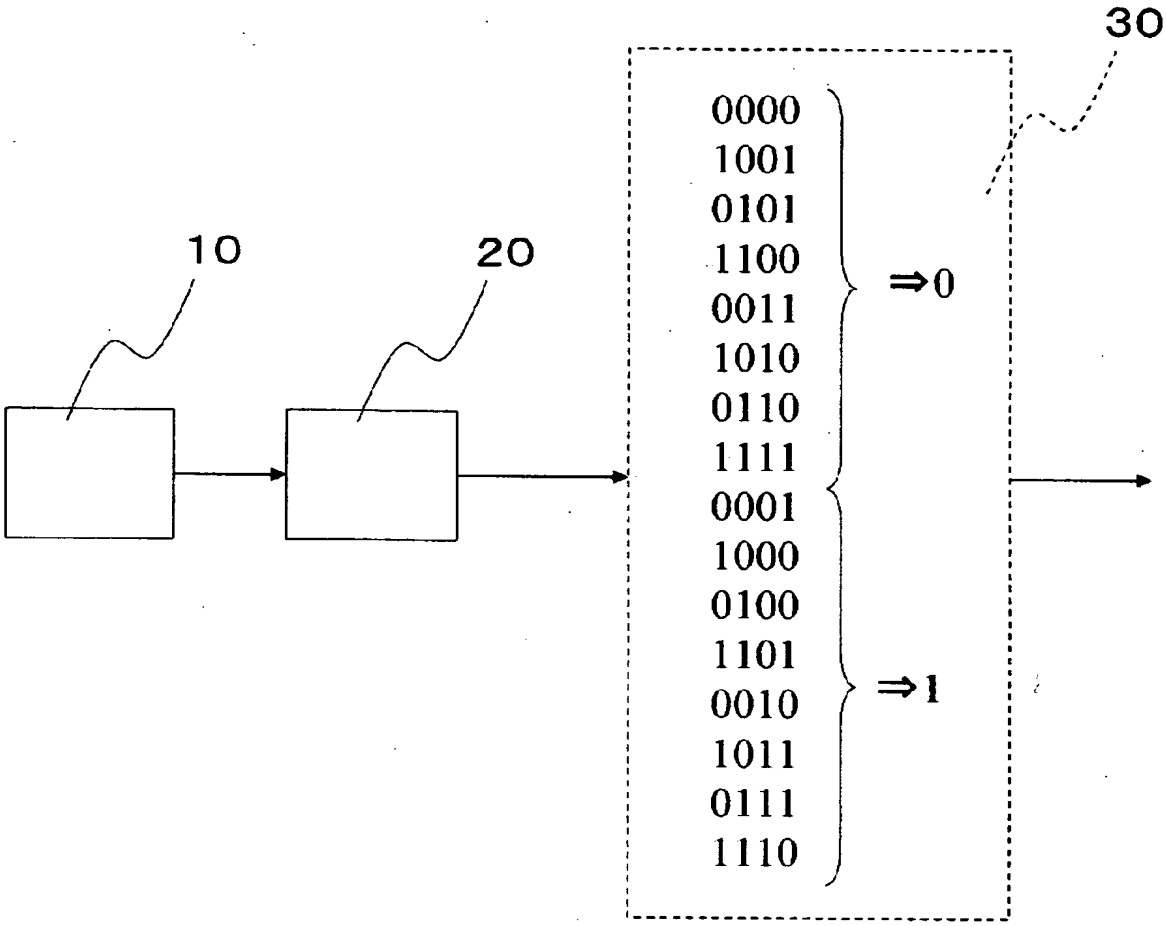
【図８】


LA1
LA2
LA3
LA4
LA5
LA6
LA7
LA8
FIPS
(モノビットテスト)
count
0
50
100
150
| average − 0.5 |
0.6
0.5
0.4
0.3
0.2
0.1
0

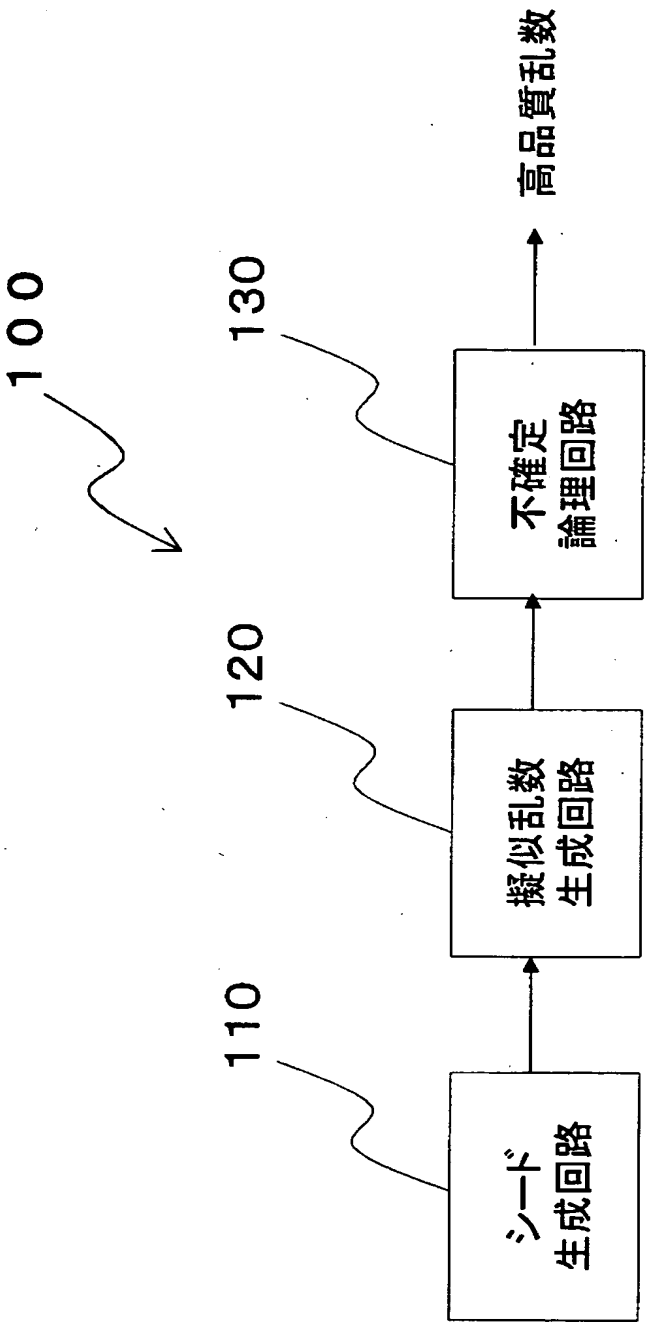
【図９】


30
0101100101101010011…
01または10⇒1
11または00⇒0を繰り返す
1ビットのシード
20
20B
20A
10
LFSR

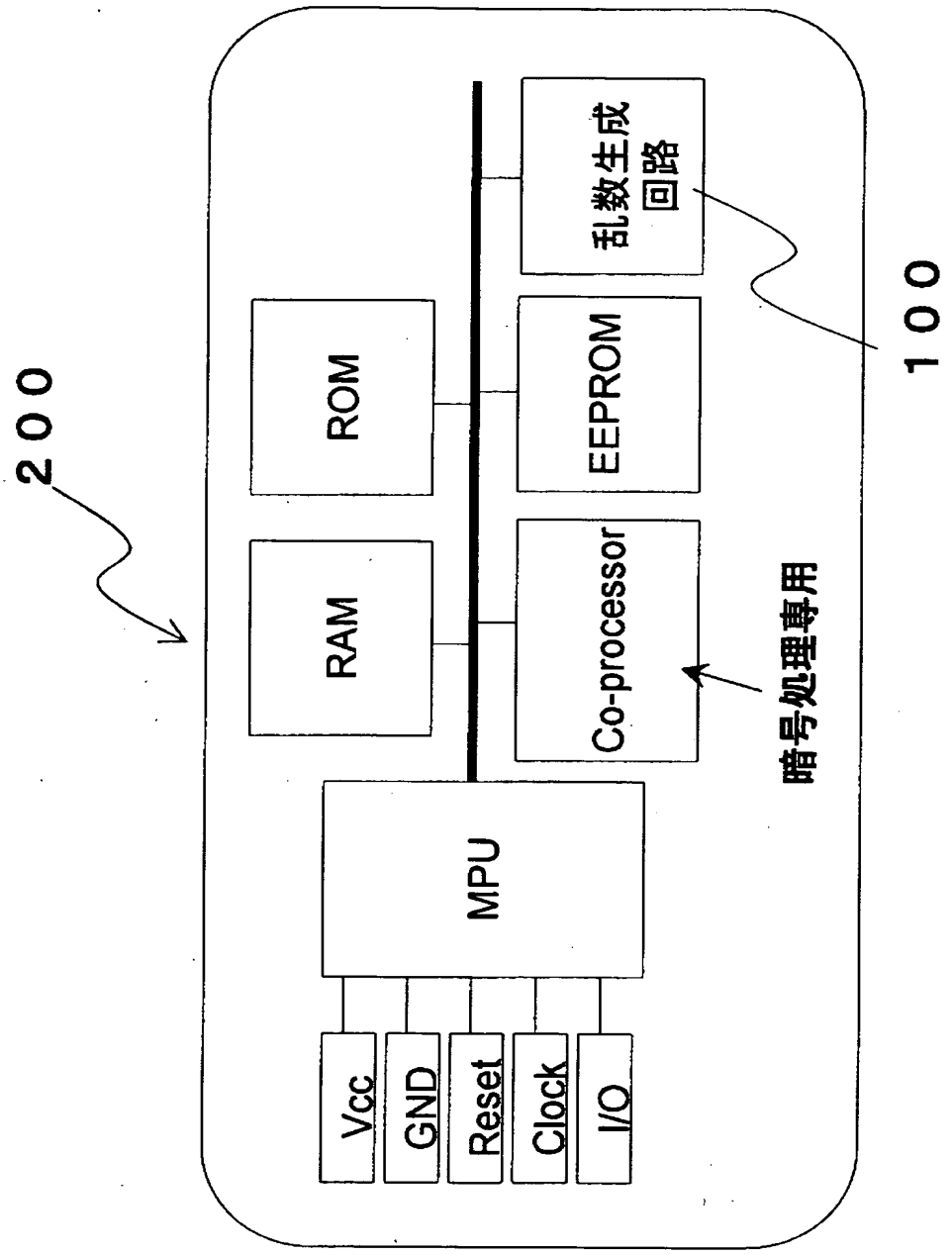
【図１０】


30
10
20
0000
1001
0101
1100
0011
1010
0110
1111
⇒0
0001
1000
0100
1101
0010
1011
0111
1110
⇒1

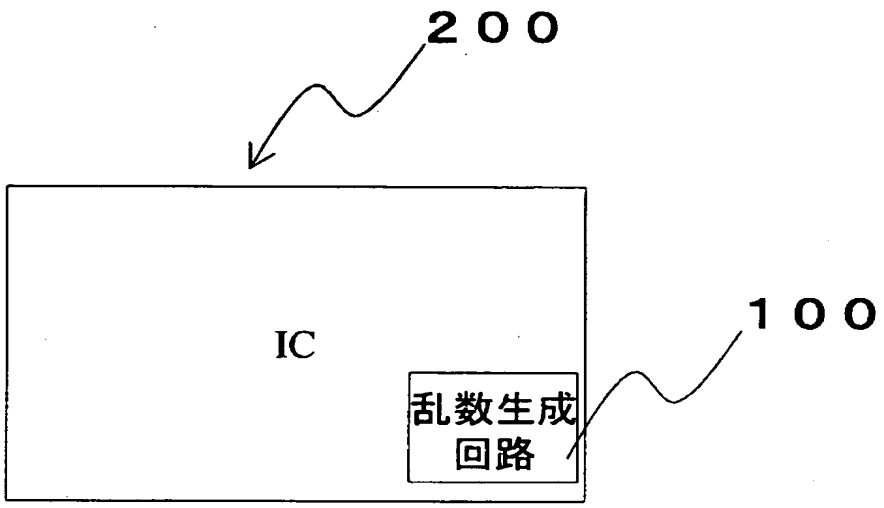
【図１１】



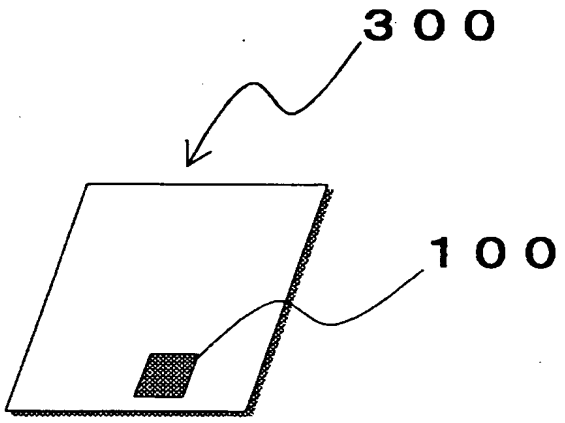
【図１２】


２００
１００
乱数生成回路
ROM
EEPROM
RAM
Co-processor
暗号処理専用
MPU
Vcc
GND
Reset
Clock
I/O

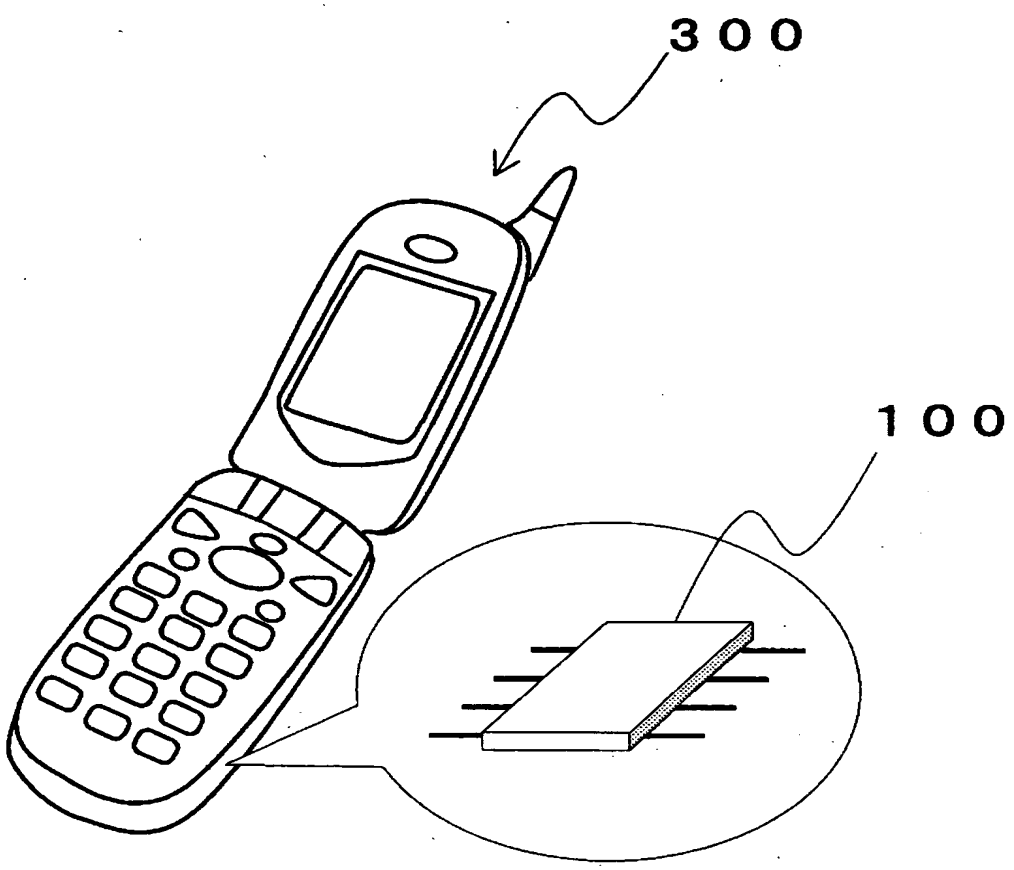
【図１３】



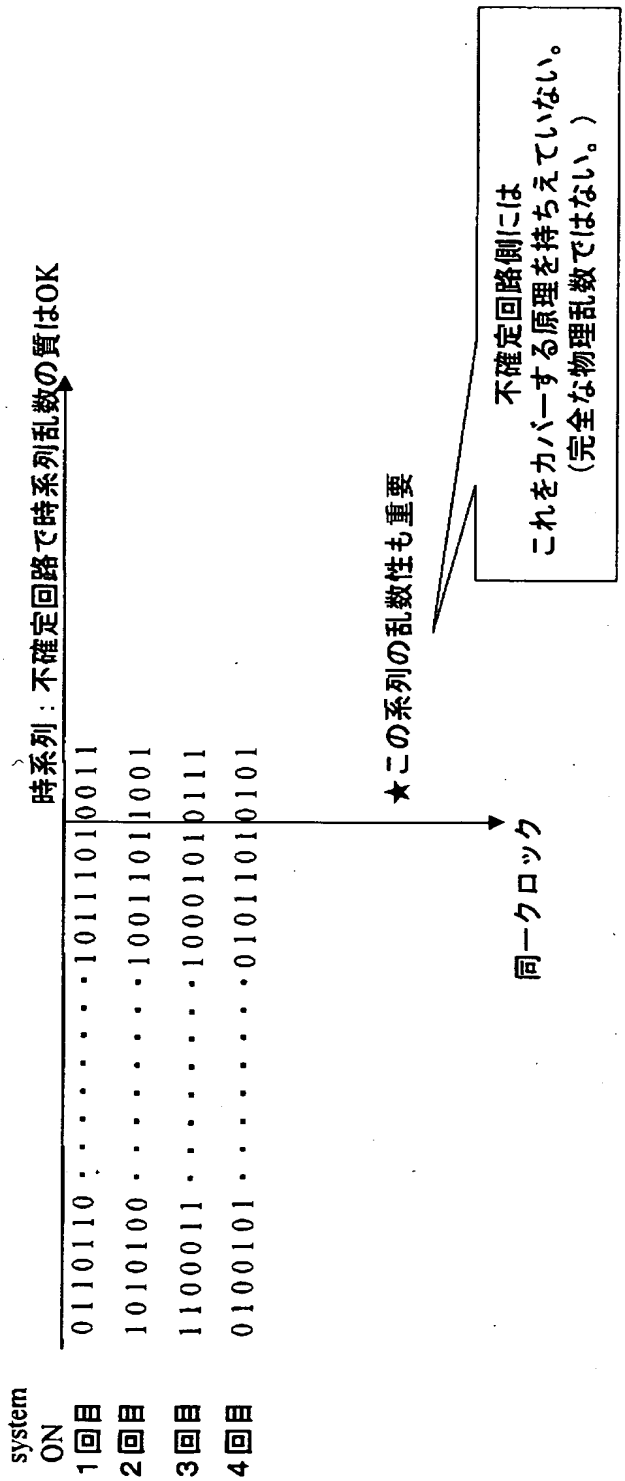
【図１４】



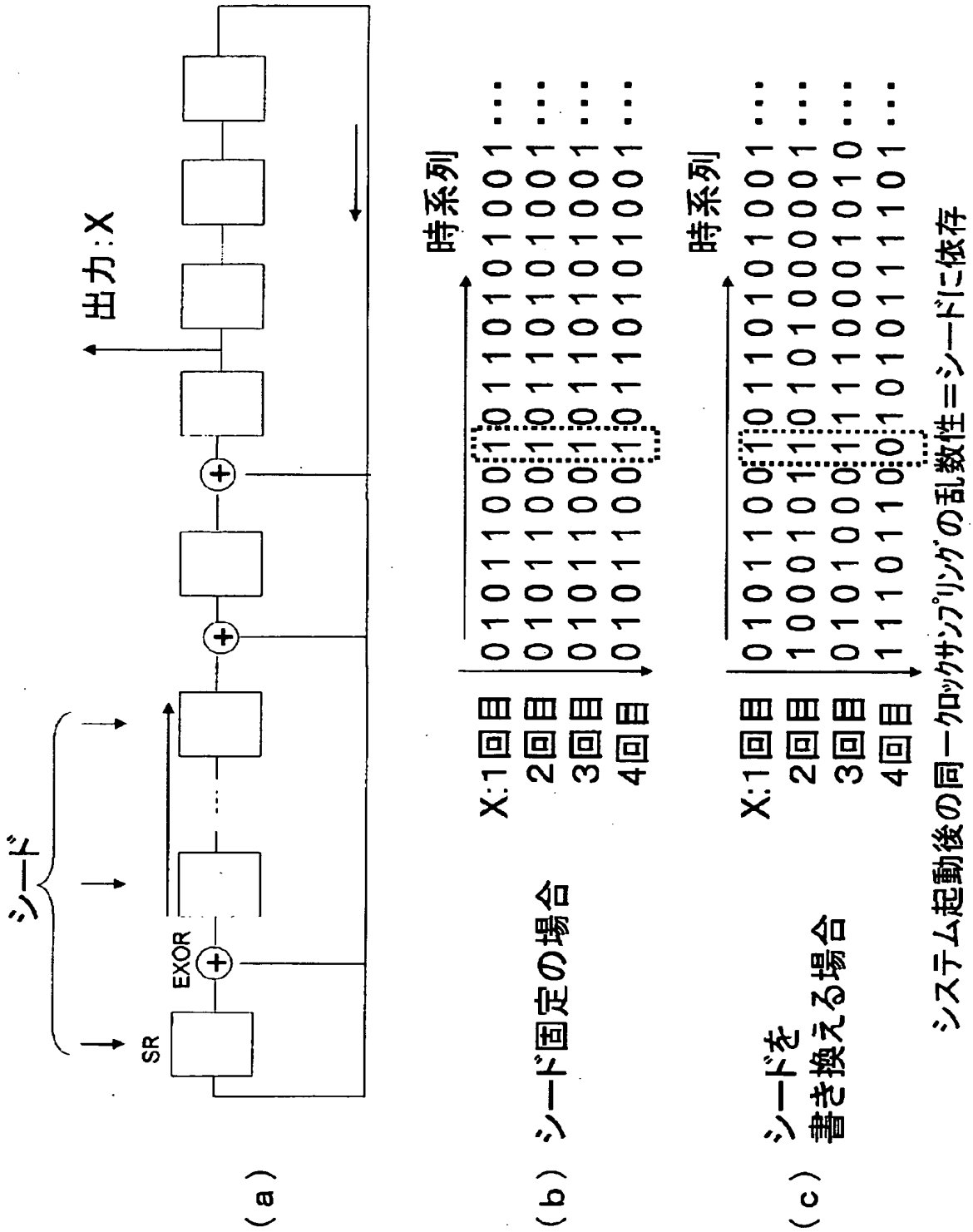
【図１５】



【図１６】


時系列：不確定回路で時系列乱数の質はOK
system ON
1回目 0110110・・・・・・・・・・10111010011
2回目 1010100・・・・・・・・・・10011010011
3回目 1100011・・・・・・・・・・10001010111
4回目 0100101・・・・・・・・・・01011010101
★この系列の乱数性も重要
同一クロック
不確定回路側には
これをカバーする原理を持ちえていない。
（完全な物理乱数ではない。）

【図１７】


出力:X
シード
EXOR
SR
（a）
時系列
X:1回目 0 1 0 1 1 0 0 1 1 0 1 1 0 1 0 1 0 0 1 1 0 0 1 ...
2回目 0 1 0 1 1 0 0 1 1 0 1 1 0 1 0 1 0 0 1 1 0 0 1 ...
3回目 0 1 0 1 1 0 0 1 1 0 1 1 0 1 0 1 0 0 1 1 0 0 1 ...
4回目 0 1 0 1 1 0 0 1 1 0 1 1 0 1 0 1 0 0 1 1 0 0 1 ...
（b）シード固定の場合
時系列
X:1回目 0 1 0 1 1 0 0 1 1 0 1 1 0 1 0 1 0 0 1 1 0 0 1 ...
2回目 1 0 0 0 1 0 1 1 0 1 1 0 1 0 1 0 0 0 0 0 0 1 1 ...
3回目 0 1 0 1 0 0 0 1 1 1 1 1 0 0 0 1 1 0 1 0 1 0 0 ...
4回目 1 1 1 0 1 1 0 1 1 0 0 1 1 0 1 0 1 1 1 1 1 0 1 ...
（c）シードを書き換える場合
システム起動後の同一クロックサンプリングの乱数性＝シードに依存

【書類名】　　要約書

【要約】

【課題】　乱数性の高いシードを生成し、かつ小型の集積回路化が可能なシード生成回路及びこれを用いた乱数生成回路、半導体集積回路、ＩＣカード及び情報端末機器を提供することを目的とする。

【解決手段】　　連続的または断続的に発振する発振回路（１０）と、前記発振回路から出力されたデジタルデータ列における「０」と「１」との出現頻度を制御して時系列データとして出力する平滑回路（２０）と、前記時系列データのうちの複数のビットを用いた演算処理により、１ビットのシードを生成する真性化回路（３０）と、を備えたことを特徴とするシード生成回路を提供する。

【選択図】　　図１

特願２００３－０１９７３２

出　願　人　履　歴　情　報

識別番号　　［０００００３０７８］

１．変更年月日　　２００１年　７月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

２．変更年月日　　２００３年　５月　９日
［変更理由］　　名称変更
住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝